УДК 004.75

ЖИЗНЕННЫЙ ЦИКЛ ТРАНЗАКЦИОННОГО ОБМЕНА МЕЖДУ УЗЛАМИ РАСПРЕДЕЛЁННОЙ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ РАСПРЕДЕЛЁННЫХ РЕЕСТРОВ

© 2020 А. С. Тороев, А. Б. Сизоненко, И. П. Павлов

Краснодарское высшее военное училище (Краснодар, Россия)

Проведён анализ жизненного цикла транзакционного обмена между узлами распределённой системы обработки данных, выявлены недостатки в его функционировании, предложен новый жизненный цикл транзакционного обмена, позволяющий снизить ресурсозатратность системы за счёт исключения «соревновательного механизма» при определении узлов-регистраторов победителей и введение «механизма назначения» на основе функционирования системы поддержки и принятия решения.

Ключевые слова: распределённый реестр, транзакция, жизненный цикл, эффективность функционирования, распределённая система, поддержка принятия решений.

Рассмотренный ранее в [1] классический жизненный цикл транзакционного обмена между узлами распределённой системы обработки данных (далее РСОД) основан на том, что узлы-регистраторы соревнуются между собой за право записи блока, который реплицируется узлам-верификаторам после исполнения алгоритма достижения консенсуса, формируя согласованный распределённый реестр, с целью получения вознаграждения, при этом приоритет транзакции зависит только от размера комиссии, которую предлагает соответствующий узел-инициализатор. В случае если РСОД создана на основе технологии распределённых реестров, но при этом не является криптовалютной системой, эффективность алгоритма, на основе которого построен данный жизненный цикл, является очень низкой в виду высокой ресурсозатратности. Кроме того, недостатком данного похода ещё является отсутствие доказательства факта формирования транзакции, так как признак корректности определяет узел-регистратор победитель (далее – УП): если предложенная транзакция не удовлетворяет его критериям, он может ее не подтвердить. А, не подтвердив необработанную транзакцию, все участники системы её удаляют, что противоречит принципу неотказуемости.

В случае ложного ветвления [3] распределённого реестра, результат исполнения алгоритма достижения консенсуса может колебаться между двумя представленными ветвями. Например, в распределённых реестрах, имеющих блочную структуру записи данных и функционирующих на основе алгоритма достижения консенсуса «Доказательство работы», если узел получает более длинную версию ветви цепи, новая ветвь будет выбрана в качестве консенсусного результата, а оригинальная ветвь будет аннулирована, что приведёт к аннулированию всех транзакций в оригинальной цепи. Таким образом, процесс подтверждения транзакций требует более детального рассмотрения.

Транзакция является подтверждённой только тогда, когда вероятность события перехода реестра R в такое состояние s в момент времени t, при котором предыдущие состояния станут недействительными, не превышает заданного порогового уровня ε. В зависимости от ценности информации или конечного продукта производители понесут разные потери в случае отмены транзакции при признании новой ветви в качестве корректной. Например, в Bitcoin важна такая характеристика, как количество подтверждений (количество блоков, записанных после блока, в который записана верифицируемая транзакция) [2]. Номер подтверждения указывает глубину транзакции в цепочке блоков и в Bitcoin на данный момент он составляет не менее пяти. Чем больше количество подтверждений, тем меньше вероятность аннулирования транзакции и тем дольше пользователю распределённого ре-

Тороев Андрей Сергеевич – Краснодарское высшее военное училище, tor_smolensk@mail.ru.
Сизоненко Александр Борисович – Краснодарское высшее военное училище, доктор техн. наук, доцент, siz_al@mail.ru.
Павлов Илья Павлович – Краснодарское высшее военное училище, pablo26rus@mail.ru.

естра придётся ожидать до начала совершения сделки. В РСОД, функционирующих в реальном времени или близкому к нему, данный алгоритм подтверждения транзакций соответственно является неприемлемым в виду низкой оперативности.

С этой целью предлагается новый жизненный цикл транзакционного обмена между узлами РСОД, который будет функционировать в режиме реального времени или близкому к нему и будет включать в себя три этапа:

1. Инициализация транзакции.
2. Запись транзакции.
3. Подтверждение транзакции.

Чтобы улучшить производительность системы данные три этапа будут функционировать в асинхронном режиме. Так как количество транзакций, инициализированных узлами сети, постоянно колеблется, скорость записи транзакций и их подтверждение должно автоматически контролироваться системой с целью сглаживания пиков и впадин, тем самым улучшая её общую пропускную способность.

Каждая транзакция будет разделяться на две части, образуя транзакционную пару. Транзакционные пары будут состоять из отправленных транзакций или «транзакций запроса», и подтверждённых транзакций или «транзакций ответа». Узел-инициализатор «A» для инициирования запроса на транзакцию «tr» формирует метку запроса записи транзакции в распределённый реестр Q(tr), которую объединяет с исходной транзакцией, подписывая своим ключом подписи (рис. 1).

Рисунок 1. Транзакция запроса на запись в распределённый реестр

Соответствующая транзакция ответа будет записываться как исходная транзакция и метка подтверждения записи транзакции в распределённый реестр A(tr), имеющая два статуса: транзакция подтверждена, транзакция отклонена. В случае если транзакция отклонена, то добавляется код причины отказа (рис. 2).

Рисунок 2. Транзакция ответа узла-регистратора о записи транзакции запроса в распределённый реестр

Если УП решит не включать какую-либо транзакцию запроса в блок, то узлы-верификаторы данный узел исключат из системы, а алгоритм достижения консенсуса запуститься заново.

В целом жизненный цикл транзакционного обмена между узлами РСОД состоит из следующих итераций:

1. Все сформированные «транзакции запроса на запись в распределённый реестр» узлами-инициализаторами в текущий момент времени ранжируются в зависимости от установленного приоритета (например, категория срочности записи транзакции) на основе метода непосредственных оценок. В зависимости от уровня приоритета предлагаемые транзакции объединяются в локальные группы транзакций (далее ЛГр Тр), образуя «пул необработанных транзакций запроса» (рис. 3):

Рисунок 3. Формирование «пула необработанных транзакций запроса»

2. Узлы-верификаторы в каждой ЛГр Тр благодаря автоматическому функционированию системы поддержки и принятия решения, назначают УП. УП проверяет корректность транзакций, формирует из них соответствующие «транзакции ответа узла-регистратора о записи транзакции запроса в распределённый реестр», объединяя их в блок на основе «дерева Меркла», подписывая заголовок блока (рис. 4).

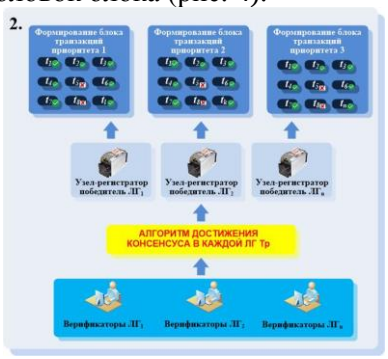

Рисунок 4. Назначение УП в каждой ЛГ Тр и верификация транзакций

3. Назначенные узлы-регистраторы победители согласуют очерёдность записи блоков транзакций в реестр, формируя раунд записи блоков. После того как блоки записаны узлами-верификаторами раунд считается завершённым, а транзакции считаются подтверждёнными (рис. 5).

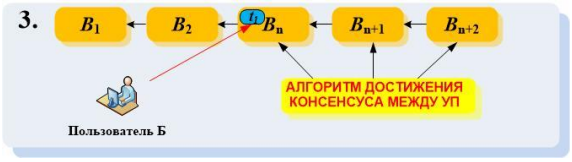

Рисунок 5. Согласование записи блоков транзакций за один раунд

Таким образом, используя предложенный жизненный цикл транзакционного обмена между узлами РСОД, узлам-регистраторам нет необходимости соревноваться между собой, так как узлы-верификаторы в каждой ЛГ Тр будут осуществлять их назначение, что значительно снизит ресурсозатратность. Объединение транзакций в локальные группы позволит уменьшить временную задержку при оповещении узлов-верификаторов, что повысит результативность и снизит вероятность ложного ветвления. С целью корректного функционирования распределённой системы обработки данных, учитывая внедрение нового жизненного цикла транзакционного обмена, требуется при проведении дальнейших исследований разработка:

1. Методики расчёта «весовых коэффициентов» узлов-регистраторов с целью функционирования системы поддержки и принятия решения;

2. Алгоритма достижения консенсуса между узлами РСОД, позволяющего назначить УП в каждой ЛГ Тр и согласовать порядок записи блоков в одном раунде.

ЛИТЕРАТУРА

1. Что такое блокчейн (blockchain). // URL:https://www.liccilip.ru/index.php/stati/blockchain.html (дата обращения: 15.09.2020).

2. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

3. Antonopoulos, A.M. Mastering Bitcoin: Unlocking Digital Cryptocurrecies; O'Reilly Media, Inc.: Newton, MA, USA, 2014.

THE LIFE CYCLE OF A TRANSACTIONAL EXCHANGE BETWEEN NODES DISTRIBUTED DATA PROCESSING SYSTEM BASED ON THE DISTRIBUTED LEDGER REGISTRIES TECHNOLOGY

© 2020 A. S. Toroev, A. B. Sizonenko, I. P. Pavlov

Krasnodar Higher Military School (Krasnodar, Russia)

An analysis of the life cycle of transactional exchange between nodes of a distributed data processing system is carried out, shortcomings in its functioning are identified, a new life cycle of transactional exchange is proposed, which allows reducing the resource consumption of the system by eliminating the "competitive mechanism" when determining the winner registration nodes and introducing a "destination mechanism" based on the functioning of the support and decision-making system.

Keywords: distributed ledger, transaction, lifecycle, operational efficiency, distributed system, decision support.